FIRST ISOMORPHISM THEOREM

$\varphi : R_1 \to R_2$ ring homomorphism

$$R_1/\ker\varphi \cong \text{Image } \varphi$$

$\downarrow$

Ring isomorphism

Pf:

$\varphi : R_1 \to R_2$

Define $\bar{\varphi} : R_1/\ker\varphi \longrightarrow \text{Image } \varphi$

as follows $\bar{\varphi}(r_1 + \ker\varphi) = \varphi(r_1)$

i) $\bar{\varphi}$ is well-defined.

Suppose $r_1 + \ker\varphi = r_1' + \ker\varphi$

$\iff r_1 - r_1' \in \ker\varphi$

So, $\varphi(r_1 - r_1') = 0$

$$\varphi(r_1) = \varphi(r_1')$$

2) $\bar{\varphi}$ preserves addition.

$$\bar{\varphi}\left(\left(r_1+\ker\varphi\right) + \left(r_2+\ker\varphi\right)\right)$$

$$= \bar{\varphi}\left((r_1+r_2) + \ker\varphi\right)$$

$$= \varphi(r_1+r_2) = \varphi(r_1)+\varphi(r_2)$$

$$= \bar{\varphi}(r_1+\ker\varphi) + \bar{\varphi}(r_2+\ker\varphi)$$

3) $\bar{\varphi}\left((r_1+\ker\varphi)(r_2+\ker\varphi)\right) = \bar{\varphi}(r_1r_2+\ker\varphi)$

$$= \varphi(r_1r_2)$$

$$= \varphi(r_1)\,\varphi(r_2)$$

$$= \bar{\varphi}(r_1+\ker\varphi)\;\bar{\varphi}(r_2+\ker\varphi)$$

4) $\bar{\varphi}(0+\ker\varphi) = \varphi(0) = 0$

5) $\bar{\varphi}(1+\ker\varphi) = \varphi(1) = 1$

Problem: Consider $R = \mathbb{Z}/3\mathbb{Z}\,[x]$.

$$I = \langle 2x^2 + x + 2 \rangle$$

a) How many elements are in the quotient ring R/I ?

b) Compute the following product $(2x+1)(x+1)$ in R/I.

c) Find the inverse of $(x+2)$ in R/I.

Fields

Defn: A *field* is a commutative ring such that every non-zero element has a multiplicative inverse.

Examples: $\mathbb{C} \supseteq \mathbb{R} \supseteq \mathbb{Q}$

Finite fields $\mathbb{Z}/p\mathbb{Z}$ p prime

$$a \neq 0 \in \mathbb{Z}/p\mathbb{Z}$$

$$ax + py = 1 \quad \text{because } \gcd(a, p) = 1$$

$$\Longleftrightarrow \quad ax = 1 \quad \text{in } \mathbb{Z}/p\mathbb{Z}$$

$$\Downarrow$$

a has a multiplicative inverse in $\mathbb{Z}/p\mathbb{Z}$

Lemma: N is a prime $\Longleftrightarrow$ $\mathbb{Z}/N\mathbb{Z}$ is a field.

Pf: $\Rightarrow$: Already shown.

$\Leftarrow$: $\mathbb{Z}/N\mathbb{Z}$ is a field.

Suppose N is not a prime. Then there exists some $a \in \mathbb{Z}/N\mathbb{Z}$ such that $a | N$, hence there are no integers x & y such that $ax + Ny = 1$

So, a has no multiplicative inverse in $\mathbb{Z}/N\mathbb{Z}$. Hence, $\mathbb{Z}/N\mathbb{Z}$ is not a field.

$\rightarrow\leftarrow$.

Integral domains

Examples: $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{Z}[x]$, ...

Defn: A commutative ring R is called an integral domain s.t whenever $ab = 0$, then either $a = 0$ or $b = 0$.

Thm: A finite integral domain is a field.

Pf: $R = \{a_1, a_2, \ldots, a_n\}$ (Assume $a_1 \neq 0$)

Consider $S = \{a_1 a_1, a_1 a_2, \ldots, a_1 a_n\} \subseteq R$

Claim: $|S| = n$

if $a_1 a_i = a_1 a_j$ for $i \neq j$

$\Rightarrow a_1 (a_i - a_j) = 0$

$\Rightarrow a_1 = 0$ or $\underset{\text{not possible}}{a_i = a_j}$

So $a_1 = 0$, contradiction.

So, $S = R$.

$\Rightarrow a_1 a_i = 1$ for some i.

Characteristic of Integral domain

Suppose $\underbrace{1+1+\cdots+1}_{n} = 0$ $\qquad n = rs$

$$\underbrace{(1+1+\cdots+1)}_{r} \underbrace{(1+1 \cdots +1)}_{s} = 0$$

either $r \cdot 1 = 0$ or $s \cdot 1 = 0$

but n is characteristic

$\Rightarrow r = n$ or $s = n$

$\Rightarrow n$ is prime.

In lecture 11 & lecture 12, there was a <u>typo</u>, instead of $\mathbb{Z}[x]$, it should say $\mathbb{Q}[x]$.

You can divide in $\mathbb{Q}[x]$, not in $\mathbb{Z}[x]$.

For example,

$$\begin{array}{r|l} & \quad 1/2 \\ \hline 2x & \quad x+1 \\ & -x \\ \hline & \quad\ 1 \end{array}$$

$$(x+1) = (2x)\left(\frac{1}{2}\right) + 1$$

$$\downarrow$$

Division in $\mathbb{Q}[x]$, not in $\mathbb{Z}[x]$.

Every ideal in $\mathbb{Q}[x]$ is principal.

This is not true in $\mathbb{Z}[x]$.

Consider the ideal generated by 2 and x.

$$I = \langle 2, x \rangle \subsetneq \mathbb{Z}[x]$$

because $1 \notin I$.

I is not principal.

If $\langle 2, x \rangle = \langle f(x) \rangle$

then $2 = f(x)\, g(x)$ for some $g(x) \in \mathbb{Z}[x]$

$\Rightarrow$ $f(x)$ must be constant.

$\Rightarrow$ $f(x) = \pm 1$ or ± 2.

If $f(x) = \pm 1$, then I is not proper.

Say $f(x) = \pm 2$, then

$$\underbrace{x = (\pm 2)\, g(x)}_{\text{not possible}}$$

So, I is not principal.

Practice Problems for Midterm 2

1) A group G of order 12 contains a conjugacy class of order 4. Prove that the center of G is trivial.

2) Let p & q be permutations. Prove that the products pq and qp have cycles of equal sizes.

3) Are the rings $\mathbb{Z}[x]/(x^2+7)$ and $\mathbb{Z}[x]/(2x^2+7)$ isomorphic?